KIBERXAVFSIZLIKDA RANSOMWARE ISHLASH MEXANIZMI VA SHIFRLASH ALGORITMLARI

МЕХАНИЗМ РАБОТЫ ВИРУСОВ-ВЫМОГАТЕЛЕЙ (RANSOMWARE) И АЛГОРИТМЫ ШИФРОВАНИЯ В КИБЕРБЕЗОПАСНОСТИ

RANSOMWARE WORKING MECHANISM AND ENCRYPTION ALGORITHMS IN CYBERSECURITY

Sobirjonov Behzod Qaxramon o‘g‘li
Farg‘ona davlat universiteti Axborot texnologiyalari kafedrasio‘qituvchisi
behzodbekqahramonovich@gmail.com
Tojimamatov Soxibjon Sherzodbek o‘g‘li
Farg‘ona davlat universiteti Axborot tizimlari va texnologiyalar yo‘nalishi
2-kurs talabasi
Sokhibaxi@gmail.com
https://doi.org/10.5281/zenodo.19909443

Annotatsiya. Ushbu maqolada ransomware turidagi zararli dasturlarning ishlash mexanizmi, ularning tizimlarga kirib borish usullari hamda ma’lumotlarni shifrlashda qo‘llaniladigan algoritmlar tahlil qilinadi. Shuningdek, zamonaviy ransomware hujumlarining rivojlanish tendensiyalari va ularning axborot xavfsizligiga ta’siri o‘rganiladi. Maqolada shifrlash texnologiyalarining ahamiyati va ularni buzishning murakkabligi yoritilib, himoya choralariga oid tavsiyalar beriladi.

Аннотация. В данной статье рассматриваются механизмы работы вредоносных программ типа ransomware, способы их проникновения в системы, а также алгоритмы шифрования, используемые для блокировки данных. Анализируются современные тенденции развития атак ransomware и их влияние на информационную безопасность. Особое внимание уделяется значению криптографических методов и сложности их взлома, а также предлагаются меры защиты.

Abstract. This article examines the working mechanisms of ransomware malware, methods of system infiltration, and encryption algorithms used to lock data. It also analyzes modern ransomware attack trends and their impact on information security. Special attention is given to the importance of cryptographic techniques and the complexity of breaking them, along with recommended protection measures.

Kalit so‘zlar: Ransomware, kiberxavfsizlik, zararli dasturlar, shifrlash algoritmlari, kriptografiya, ma’lumotlarni bloklash, AES, RSA, tarmoq hujumlari, axborot xavfsizligi

Ключевые слова: Ransomware, кибербезопасность, вредоносное ПО, алгоритмы шифрования, криптография, блокировка данных, AES, RSA, сетевые атаки, информационная безопасность

Keywords: Ransomware, cybersecurity, malware, encryption algorithms, cryptography, data encryption, AES, RSA, network attacks, information security

Kirish

So‘nggi yillarda kiberxavfsizlik sohasida ransomware turidagi hujumlar keskin ortib bormoqda. Ushbu zararli dasturlar foydalanuvchi yoki tashkilot ma’lumotlarini shifrlab, ularni qayta tiklash evaziga to‘lov talab qiladi. Ransomware hujumlari ko‘plab tashkilotlarga katta moliyaviy zarar yetkazmoqda va axborot tizimlarining ishonchliligiga jiddiy tahdid solmoqda.

Ransomware dasturlari odatda fishing xatlari, zararli fayllar yoki tizimdagi zaifliklardan foydalanish orqali tarqaladi. Ular tizimga kirgach, muhim fayllarni aniqlab, kuchli kriptografik algoritmlar yordamida shifrlaydi. Shu sababli bunday hujumlardan himoyalanish uchun nafaqat xavfsizlik choralarini, balki kriptografiya asoslarini ham chuqur tushunish zarur.

Mazkur maqolada ransomware ishlash mexanizmi, uning asosiy bosqichlari hamda shifrlash algoritmlarining roli atroflicha tahlil qilinadi.

Mazkur amaliy ishda ransomware dasturlarining ishlash mexanizmi bosqichma-bosqich tahlil qilindi. Dastlab, zararli dastur tizimga kirish yo‘llari o‘rganildi. Aniqlanishicha, ransomware ko‘pincha fishing xabarlari, zararli yuklamalar yoki xavfsizlikdagi zaifliklar orqali foydalanuvchi qurilmasiga kiradi.

Tizimga kirgandan so‘ng, dastur o‘zini yashirin holatda ishga tushiradi va foydalanuvchiga sezilmasdan faoliyat yuritadi. Keyingi bosqichda u tizimdagi muhim fayllarni aniqlaydi va ularni shifrlash jarayonini boshlaydi. Shifrlashda ko‘pincha simmetrik va assimmetrik algoritmlar birgalikda qo‘llaniladi. Masalan, fayllarni tez shifrlash uchun AES algoritmi ishlatilsa, kalitni himoyalash uchun RSA algoritmidan foydalaniladi.

Shifrlash jarayoni yakunlangach, foydalanuvchiga maxsus xabar chiqariladi va ma’lumotlarni tiklash uchun to‘lov talab qilinadi. Bu to‘lov odatda kriptovalyuta orqali amalga oshiriladi.

Tahlil davomida ransomware dasturlarining murakkabligi va ularni aniqlashning qiyinligi kuzatildi. Ayniqsa, kuchli shifrlash algoritmlari sababli fayllarni kalitsiz tiklash deyarli imkonsiz hisoblanadi. Shu sababli asosiy e’tibor bunday hujumlarning oldini olishga qaratilishi kerak.

XULOSA

Mazkur maqolada ransomware zararli dasturlarining ishlash mexanizmi va shifrlash algoritmlarining ahamiyati keng yoritildi. Tahlillar shuni ko‘rsatdiki, ransomware hujumlari zamonaviy kiberxavfsizlikka jiddiy tahdid solmoqda va ularning asosiy kuchi kuchli kriptografik algoritmlarga asoslangan.

Shuningdek, ransomware hujumlarining oldini olish ularni bartaraf etishdan ko‘ra samaraliroq ekanligi aniqlandi. Shu sababli foydalanuvchilarni xabardor qilish, tizimlarni muntazam yangilab borish va zaxira nusxalar yaratish muhim ahamiyat kasb etadi.

Adabiyotlar, References, Литературы:

1. Stallings W. — Cryptography and Network Security. Pearson, 2017.
2. Anderson R. — Security Engineering. Wiley, 2020.
3. NIST — Guide to Malware Incident Prevention.
4. Kaspersky Lab — Ransomware Research Reports.
5. Symantec — Internet Security Threat Report.
6. OWASP — Top 10 Security Risks.